AD-A053 039 SYSTEM DEVELOPMENT CORP SANTA MONICA CALIF F/G 9/2
SOFTWARE ACQUISITION MANAGEMENT GUIDEBOOK: VALIDATION AND CERTI--ETC(U)
AUG 77 A M SKRUKRUD, N E WILLMORTH F19628-76-C-0236
UNCLASSIFIED SDC-TM-5772/003/02 ESD-TR-77-326 NL

1 OF 1
AD
A053039

END
DATE
FILMED
5-78
DDC

ESD-TR-77-326

AD A053039

SOFTWARE ACQUISITION MANAGEMENT GUIDEBOOK: VALIDATION AND CERTIFICATION

System Development Corporation
2500 Colorado Avenue
Santa Monica, CA 90406

August 1977

AD No.
DDC FILE COPY

DDC
APR 24 1978

Approved for Public Release;
Distribution Unlimited.

DEPUTY FOR COMMAND AND MANAGEMENT SYSTEMS
ELECTRONIC SYSTEMS DIVISION
HANSCOM AIR FORCE BASE, MA 01731

LEGAL NOTICE

When U. S. Government drawings, specifications or other data are used for any purpose other than a definitely related government procurement operation, the government thereby incurs no responsibility nor any obligation whatsoever; and the fact that the government may have formulated, furnished, or in any way supplied the said drawings, specifications, or other data is not to be regarded by implication or otherwise as in any manner licensing the holder or any other person or conveying any rights or permission to manufacture, use, or sell any patented invention that may in any way be related thereto.

OTHER NOTICES

Do not return this copy. Retain or destroy.

This technical report has been reviewed and is approved for publication.

William J. White

WILLIAM J. WHITE, Capt, USAF
Project Engineer

John C. Mott-Smith

JOHN C. MOTT-SMITH
Project Manager

John T. Holland

JOHN T. HOLLAND, Lt Col, USAF
Chief, Techniques Engineering Division

FOR THE COMMANDER

Stanley J. Dereska

STANLEY J. DERESKA, Colonel, USAF
Deputy Director, Computer Systems Engineering
Deputy for Command and Management Systems

SECURITY CLASSIFICATION OF THIS PAGE *(When Data Entered)*

(19) **REPORT DOCUMENTATION PAGE**

READ INSTRUCTIONS BEFORE COMPLETING FORM

(18) REPORT NUMBER: ESD-TR-77-326

2. GOVT ACCESSION NO.

(9) 3. RECIPIENT'S CATALOG NUMBER: Technical rept.

4. TITLE *(and Subtitle)*

(6) SOFTWARE ACQUISITION MANAGEMENT GUIDEBOOK: VALIDATION AND CERTIFICATION

5. TYPE OF REPORT & PERIOD COVERED

(14) 6. PERFORMING ORG. REPORT NUMBER: SDC-TM-5772/003/02

(10) 7. AUTHOR(s): Allan M. Skrukrud; Norman E. Willmorth

(15) 8. CONTRACT OR GRANT NUMBER(s): F19628-76-C-0236

9. PERFORMING ORGANIZATION NAME AND ADDRESS
System Development Corporation
2500 Colorado Avenue
Santa Monica, CA 90406

10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS

11. CONTROLLING OFFICE NAME AND ADDRESS
Deputy for Command and Management Systems
Electronic Systems Division
Hanscom AFB, MA 01731

(11) 12. REPORT DATE: August 1977

13. NUMBER OF PAGES: 43

14. MONITORING AGENCY NAME & ADDRESS *(if different from Controlling Office)*

(12) 51 p.

15. SECURITY CLASS. *(of this report)*: UNCLASSIFIED

15a. DECLASSIFICATION/DOWNGRADING SCHEDULE: N/A

16. DISTRIBUTION STATEMENT *(of this Report)*

Approved for Public Release; Distribution Unlimited.

17. DISTRIBUTION STATEMENT *(of the abstract entered in Block 20, if different from Report)*

DDC
APR 24 1978
F

18. SUPPLEMENTARY NOTES

19. KEY WORDS *(Continue on reverse side if necessary and identify by block number)*

CERTIFICATION
SOFTWARE ACQUISITION MANAGEMENT
SYSTEM SPECIFICATION VALIDATION
SYSTEM VALIDATION
VALIDATION

20. ABSTRACT *(Continue on reverse side if necessary and identify by block number)*

This report is one of a series of Software Acquisition Management Guidebooks which provide information and guidance for ESD Program Office personnel who are charged with planning and managing the acquisition of command, control, and communications system software procured under Air Force 800 series regulations and related software acquisition management concepts. It provides a review of the validation and certification practices and procedures employed by industry and set forth in relevant

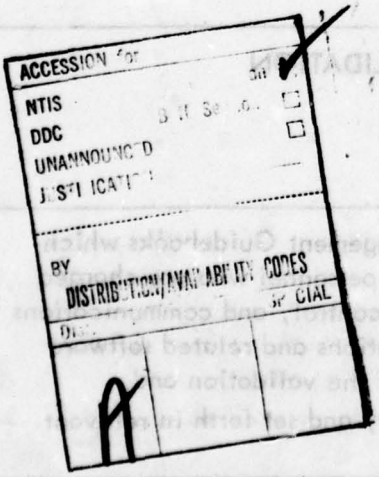
DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

SECURITY CLASSIFICATION OF THIS PAGE *(When Data Entered)*

339 900

20. ABSTRACT (Con't)

Department of Defense and Air Force regulations, specifications, and standards. It (1) defines the terms "validation" and "certification", and distinguishes them from the term "verification" as applied to software; (2) describes the software-related planning, system engineering, and testing activities carried out by the Program Office which lead to system validation and certification; (3) provides guidance in planning and executing those software-related activities necessary to successfully achieve system validation and certification; (4) references other guidebooks in this series which provide more detailed information on the specific software techniques and tools required in system validation and certification; (5) references the appropriate Department of Defense and Air Force regulations, specifications, and standards that establish the basis for system validation and certification.



PREFACE

The Validation and Certification guidebook is one of a series of Software Acquisition Management (SAM) Guidebooks intended to help ESD Program Office personnel in the acquisition of embedded software for command, control and communications systems. The contents of the guidebooks will be revised periodically to reflect changes in software acquisition policies and practices as well as feedback from guidebook users.

This report was prepared by System Development Corporation (SDC) under the direction of the Computer Systems Engineering Directorate (MCI) of the Electronic Systems Division (ESD), Air Force Systems Command (AFSC). Contributions were made by: Mr. J. Mott-Smith and Captain W. White (ESD/MCI); Mr. J. Trachtenberg (AFALD/AQE); Mr. M. Landes (RADC/ISI); Mr. M. Mleziva (ESD/EN); Mr. M. Zymaris (ESD/DRT); Mr. D. Peterson (The MITRE Corporation); Captain J. Haughney (AFCS/LO); and Mr. G. Gehlauf (AFLC/LOAK).

The Software Acquisition Management Guidebook series is currently planned to cover the following topics (National Technical Information Service accession numbers for those already published are shown in parentheses):

Regulations, Specifications and Standards (AD-A016401)

Contracting for Software Acquisition (AD-A020444)

Monitoring and Reporting Software Development Status (AD-A016488)

Statement of Work Preparation (AD-A035924)

Reviews and Audits

Computer Program Configuration Management

Computer Program Development Specification (Requirements Specification)

Software Documentation Requirements (AD-A027051)

Verification

Validation and Certification

Overview of the SAM Guidebooks

Software Maintenance

Software Quality Assurance

Software Cost Estimation and Measurement

Software Development and Maintenance Facilities (AD-A038234)

Life Cycle Events (AD-037115)

(Page 2 blank)

TABLE OF CONTENTS

	Page
PREFACE	1
SECTION 1 - INTRODUCTION	5
1.1 Purpose	5
1.2 Validation, Certification, and Verification Defined	5
1.2.1 Validation	6
1.2.2 Certification	8
1.2.3 Verification	8
1.3 Relationship to Other Guidebooks	9
1.4 Contents	10
SECTION 2 - VALIDATING THE SYSTEM SPECIFICATION	11
2.1 Objectives	11
2.2 Validation Considerations	11
SECTION 3 - INTEGRATING THE SOFTWARE	17
3.1 Objectives	17
3.2 Software Integration Considerations	17
SECTION 4 - THE SOFTWARE ASPECTS OF SYSTEM VALIDATION	21
4.1 Objectives	21
4.2 Planning for System Validation	21
4.2.1 PMP Considerations	21
4.2.2 TEMP Considerations	22
4.2.3 System Specification Considerations	23
4.2.4 System DT&E Plan Considerations	25
4.3 Monitoring Activities	26
4.4 System DT&E Conduct	27
SECTION 5 - PLANNING FOR CERTIFICATION	29
5.1 Plans	29
5.2 Turnover and Transfer	31
5.3 OT&E Support Activities	33

TABLE OF CONTENTS (cont'd)

	Page
SECTION 6 - MANAGEMENT OF SYSTEMS UNDER TEST	35
6.1 Maintenance of Test Documentation	35
6.2 Program Libraries	36
6.3 Test Status Reports	36
6.4 Software Problem Reporting and Correction	37
6.4.1 Reporting Problems	37
6.4.2 Problem Disposition	38
6.4.3 Responsibility for Diagnosis	38
6.4.4 Responsibility for Correction	38
6.4.5 Correction Control	39
APPENDIX A - GLOSSARY	41
APPENDIX B - BIBLIOGRAPHY	47
APPENDIX C - REFERENCES	49

SECTION 1 - INTRODUCTION

1.1 PURPOSE

The Validation and Certification guidebook is designed to assist Program Office personnel in planning and managing the implementation of validation and certification concepts and requirements as they relate to military command control, and communications system software acquisition management. It provides a review of the validation and certification practices and procedures employed by industry and set forth in relevant Department of Defense and Air Force regulations, specifications, and standards.

This document recognizes and is compatible with Air Force 800-series regulations and related concepts.

Validation and certification are two major system acquisition cycle activities which have software implications. This guidebook:

- Defines the terms "validation" and "certification", and distinguishes them from the term "verification" as applied to software.
- Describes the software-related planning, system engineering, and testing activities carried out by the Program Office (PO) which lead to system validation and certification.
- Provides guidance in planning and executing those software-related activities necessary to successfully achieve system validation and certification.
- References other guidebooks in this series which provide more detailed information on the specific software techniques and tools required in system validation and certification.
- References the appropriate Department of Defense (DoD) and Air Force Regulations, Specifications, and Standards (RSSs) that establish the basis for system validation and certification.

1.2 VALIDATION, CERTIFICATION, AND VERIFICATION DEFINED

Validation is system oriented. It begins with the System Specification and concludes at the end of System Development Test and Evaluation (DT&E).

Certification is a user-oriented, system-level activity and occurs during Operational Test and Evaluation (OT&E).

Verification is Computer Program Configuration Item (CPCI) oriented. It begins with system and software engineering activities, which lead to CPCI definitions and to the CPCI Development Specification, and ends with the qualification of the CPCI.

Figure 1 illustrates validation, certification, and verification, within the context of this guidebook series by showing the successive development of specifications from the System Specification to the CPCI Product (Part II) Specification. The following paragraphs further define the terms validation, certification, and verification within this context. These definitions also serve to distinguish the subject matter of this guidebook from that of the Verification guidebook.

1.2.1 Validation

Validation, as used in this guidebook series, comprises those evaluation, integration, and test activities carried out at the system level to ensure that the finally developed system satisfies the requirements of the System Specification. While the validation process has significant software implications, a software validation process, distinct from the system validation process, cannot be isolated since all evaluation and test activities that make up validation are focused at the system level.

Specific validation tasks include:

- System engineering activities carried out to ensure that the requirements in the System Specification accurately respond to the operational needs called for in the Required Operational Capability (ROC) [validating the System Specification] - see Section 2.
- Configuration Item (CI) integration activities (including CPCI integration) carried out to assemble and check out previously qualified CIs as a fully functioning system [installation and checkout] - see Section 3.
- The software aspects of system validation carried out during System DT&E and Initial Operational Test and Evaluation (IOT&E) to demonstrate that the completed system meets the requirements called for in the System Specification [validating the system] - see Section 4.

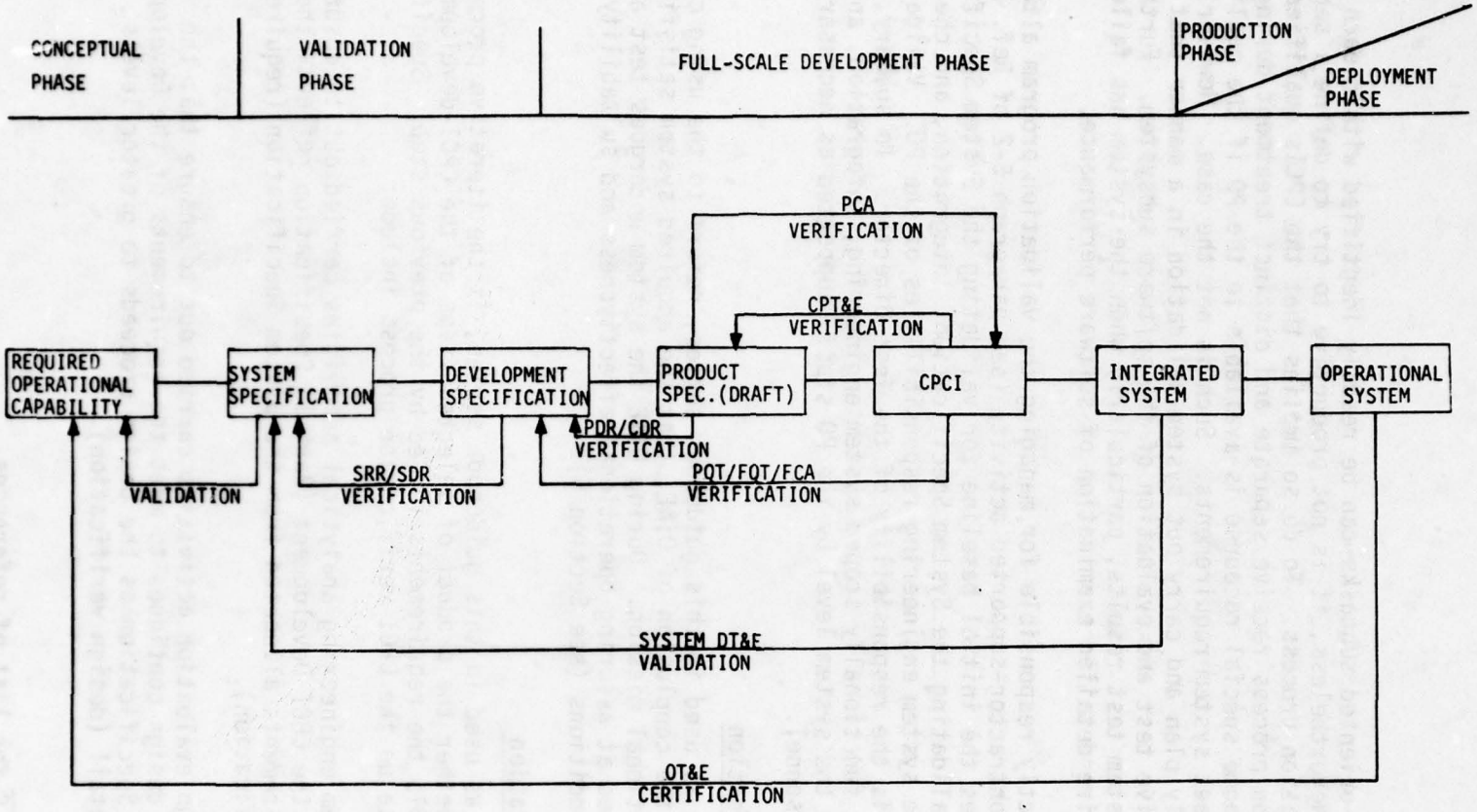


Figure 1. The Scope of Validation, Certification and Verification

Major software-oriented subtasks can be readily identified within each of the above tasks. Nevertheless, it is not productive to try to define a separate software validation process. To do so implies that the CPCIs qualified during the verification process receive separate and distinct treatment during System DT&E and that some special recourse is available to the PO if the qualified CPCIs do not meet system requirements. Such is not the case. However, the PO should certainly plan and carry out system validation in a manner that ensures the comprehensive test and evaluation of the software subsystem. Furthermore, analysis of system test results, particularly when the system has failed the test, may require detailed examination of software performance.

The PO is directly responsible for managing the validation program although it is usually a contractor-supported activity (see paragraph 5-2 of Ref. [3])*. The ROC provides the initial baseline for validating the System Specification. The tasks of validating the System Specification, integration, and checkout fall within the system engineering responsibilities of the PO. Validating the system itself is the responsibility of the Test Director. In summary, validation comprises functionally scoped system engineering, integration, and testing carried out at the system level by the PO staff, supported as necessary by contractor personnel.

1.2.2 Certification

Certification, as used in this guidebook series, refers to the using command's agreement, at the conclusion of OT&E, that the acquired system satisfies its intended operational mission. During OT&E the system undergoes test and evaluation aimed at assuring operational effectiveness and suitability under operational conditions (see Section 5).

1.2.3 Verification

Verification, as used in this guidebook series, is the iterative process of determining whether the product of selected steps of the CPCI-development process fulfills the requirements levied by the previous step. Specific task areas that make up the CPCI verification process include:

- System engineering analytical activities carried out to ensure that the CPCI Development (Part I) Specification reflects the requirements allocated from the System Specification (requirements verification).

- Design evaluation activities carried out to ensure that the CPCI design continues to meet the requirements of the Development Specification as the design proceeds to greater levels of detail (design verification).

*See Appendix C for list of references.

- Informal testing of the CPCI and its components [Computer Program Test and Evaluation (CPT&E)] carried out by the contractor at his discretion to assist in development, provide visibility of progress, and prepare for formal testing (computer program verification).

- Formal testing of the CPCI [Preliminary Qualification Test (PQT) and Formal Qualification Test (FQT)] carried out by the contractor in accordance with Air Force-approved test plans and procedures to verify that the CPCI fulfills the requirements of the Development Specification and to provide the basis for CPCI acceptance by the Air Force.

The CPCI contractor is responsible for most of the CPCI verification tasks although the PO monitors and controls his performance by approving the Development Specification, participating in design reviews, approving the test documentation, witnessing the execution of formal tests, and approving the qualification test results. The CPCI Development Specification provides the baseline against which the CPCI is verified (qualified). Verification has the basic Quality Assurance (QA) objective of ensuring that the developing CPCI retains its equivalency to the current baselined specification as design and development proceed to increasingly lower levels of detail. Thus at the System Design Review (SDR), the contractor must show that the requirements to be included in the Development Specification are traceable to the System Specification. At PDR and CDR the contractor must demonstrate the equivalency of each successively detailed design to the baselined Development Specification. During qualification (FQT) the contractor must demonstrate that the coded programs meet the Development Specification requirements. In summary, verification comprises system engineering and computer programming-oriented evaluation and testing activities carried out at the Computer Program Component (CPC) and CPCI levels by the CPCI contractor and monitored by the PO.

1.3 RELATIONSHIP TO OTHER GUIDEBOOKS

This guidebook does not stand alone in providing information on validation and certification. The Overview guidebook establishes a frame of reference for the whole guidebook series. The Verification guidebook and Reviews and Audits guidebook provide more detail on System Requirements Reviews (SRRs) and SDRs. The Software Documentation Requirements guidebook covers test planning and reporting documentation. The Verification guidebook contains descriptions of test tools. Finally, the Configuration Management guidebook provides information on configuration management procedures related to validation, in particular on configuration control during DT&E. An effective validation and certification program must incorporate the concepts presented in all of these guidebooks.

1.4 CONTENTS

The subsequent contents of this guidebook include four sections and two appendixes, as follows:

- Section 2 - Validating the System Specification. Discusses in detail the activities involved in ensuring that the System Specification accurately reflects the mission requirements of the system.
- Section 3 - Integrating the Software. Addresses in detail the activities involved in integrating and checking out the CPCIs prior to System DT&E.
- Section 4 - The Software Aspects of System Validation. Describes the software-related activities involved in planning and executing a comprehensive System DT&E program.
- Section 5 - Planning for Certification. Discusses the PO's software-related responsibilities concerning system turnover, transfer of management responsibility, and system certification.
- Section 6 - Management of Systems Under Test. Addresses maintenance of test documentation, program libraries, test status reports, and software problem reporting and correction.
- Appendix A - Glossary. Defines terms and acronyms used in this guidebook.
- Appendix B - Bibliography. Provides a list of RSSs, technical books, and papers that are particularly relevant to the subjects of validation and certification.
- Appendix C - References. Presents a list of numbered references used in this guidebook, e.g., "see Ref. [1]."

SECTION 2 - VALIDATING THE SYSTEM SPECIFICATION

This section addresses those Conceptual and Validation Phase activities which lead to the generation and updating of the System Specification and the establishment of those performance requirements which, when authenticated, form the Functional Baseline for the system. The system design evolves as a result of system engineering activities and allocation of system functions to hardware or software.

2.1 OBJECTIVES

During the Conceptual Phase, the PO seeks to develop a System Specification which (1) satisfies the mission requirements in the most cost effective manner and (2) provides the contract baseline for the Validation Phase. In accomplishing these goals, the PO may be pressured to develop the ultimate system* on the one hand and to reduce development risk and cost on the other. However, the PO's overall concern is the successful turnover and transfer of the system, which requires a careful assessment of each System Specification requirement to determine its impact on these objectives. Software requirements necessitate particular scrutiny since an unrealistic requirement, such as an unnecessarily high throughput or an unreasonably fast response time may have a significant impact on development cost and schedule. In addition, the lack of attention to such items as growth requirements, flexibility, and software support during operations may well result in a system which is functionally satisfactory but is difficult to operate and maintain. (See Refs. [8 & 9] for information regarding support considerations.)

2.2 VALIDATION CONSIDERATIONS

The validation of the System Specification is an ongoing process which occurs during both the Conceptual and Validation Phases. During the Conceptual Phase, the initial System Specification is developed and baselined as the contract specification for the Validation Phase. In reviewing the System Specification, the PO should assure that the following software-related considerations are incorporated:

- The specification provides a complete basis for translation into quantitative and qualitative requirements statements for the CPCI Development Specification.
- If a mission scenario is included, it is detailed enough to provide a basis for system testing. In addition, plans should have been developed for providing scenario inputs or a simulation capability for testing should have been specified. The plans should be compatible with the using command's Operational Employment Plan (see paragraph 2-10 of Ref. [7]).

*By the using command.

- System engineering trade studies have been performed to support the viability of the requirements and to identify and reduce any risk areas. For example the studies should show that estimated costs and schedules are compatible with known approaches to satisfying the performance, capacity, and throughput requirements of the System Specification.

- All the requirements stated in the ROC have been addressed. Frequently, the System Specification does not include all the ROC requirements because some of the requirements may not have state-of-the-art solutions, may be too costly to implement, or may adversely impact program schedules. However, the validation effort should ensure that documented evaluations are available to support any ROC requirements which were not included.

- It is specified whether the system is single- or multi-site. These considerations may affect hardware/software tradeoffs and support software requirements. A single-site system may be most economically procured by emphasizing lower software development costs at the expense of additional hardware costs. A multi-site system may be most economically procured by reducing the Production Phase hardware costs at the expense of higher software development costs. For example, for a single site it may be less expensive and incur lower risk to buy sophisticated display consoles containing built-in processing capabilities. As the number of display consoles or the number of sites increases, it becomes more advantageous and less costly to incorporate the display processing capabilities in the software.

- The expected level of change in the system and the response time required for implementing changes have been considered. This factor affects hardware/software tradeoffs and flexibility and growth requirements. It may also affect centralized versus decentralized maintenance capability requirements (see Refs. [8 & 9]). For instance, an extremely stable system might be hardwired to minimize production costs, but this approach incurs penalties in the form of delays when modifications are required. Conversely, a system requiring rapid modification at any of its sites is best developed with maximum use of software and on-site modification and support capabilities.

- Any Government Furnished Equipment (GFE) or software is specified and is appropriate for the intended application. A GFE processor, which is not designed for this particular application, may have insufficient storage, inadequate throughput, insufficient

growth capacity, inappropriate instruction set, or lack of adequate support software [e.g., lack of a resident compiler for the Higher Order Language (HOL) selected]. This may require the development of exceedingly complex software to meet user requirements. Similarly, the specification of inappropriate GFE software may result in increased processor timing or loading problems, increased application software development requirements, or costly modification. If GFE is specified, then the Government assumes the risk if the items are not satisfactory for the task.

- All requirements are stated in quantitative and qualitative terms that are testable. That is, the specification must state requirements whose achievement can be measured in a clear and unambiguous manner. These requirements may relate to a scenario or set of conditions which must be met before the measurement can take place. When reviewing each functional requirement, the PO should determine if enough information exists for design and testing to occur. Any item which is left open to subjective judgement is a potential problem.

- All requirements are really performance requirements rather than design constraints unless sufficient system engineering and analysis have been accomplished to justify their inclusion as design constraints. Specification of specific design requirements, rather than performance requirements, puts the risk in the hands of the Government if the design is inadequate.

- Software support and modification requirements are at least initially identified. If not, costly additions to the system may result both before certification and during operations. Support tools, facilities, and the recruitment and training of support personnel should all be addressed (see Ref. [9]).

- System availability requirements are consistent with the system's intended operation and will not require unnecessarily expensive hardware or software. Overly restrictive requirements for system recovery and loss of data may result in unnecessary software development costs. Particular attention should be paid to interfacing systems and their ability to resend data where required to aid in system recovery. Accountability of incoming data on a message basis is cheaper than accountability on a character or bit basis, if the source can accommodate this method.

- External system interface definitions are accurate and complete. Too many systems have been developed and tested to erroneous interface specifications. Interface problems often arise late in the Full-Scale Development Phase when an attempt is made to

integrate the system, a time when resources are being consumed at a rapid rate and schedules are very tight. It is better to define an interface as a "To Be Defined" (TBD) and to require its definition later than to put in data that has not been completely verified.

- Paragraph 3.3.8 (see Ref. [10]) includes any required software design standards, identifies prescribed programming languages, and states any other software design constraints.

- Requirements, as stated in the System Specification, provide the operational capabilities stated in the ROC. This effort should be ongoing during both the Conceptual and Validation Phases with strong participation by the eventual user. The use of simulation to model major areas should be considered when there are alternative methods of providing a particular capability. Trade studies to validate the most cost effective method of providing a given capability should be conducted and presented at the SRR. A complete understanding of the operational environment and procedures will often lead to the identification of least-cost solutions to providing a given capability. The major thrust should be to assure that the requirements in the System Specification will satisfy all ROC requirements in the most cost-effective manner when they are implemented in the users operational environment.

To assure coverage of the above considerations in the System Specification, the PO should evaluate each System Specification requirement against the following standards:

- Is this requirement really a performance requirement?

- Is this performance requirement stated in a manner which will support unambiguous design and test?

The initial System Specification produced during the Conceptual Phase forms the contractual baseline for Validation Phase efforts. If a contractor (or contractors) is utilized for the Validation Phase, a series of System Requirements Reviews (SRRs) should be scheduled. The first of these should be held shortly after the beginning of the Validation Phase to assure that the contractor completely understands the requirements contained in this specification. Subsequent reviews should be scheduled to cover all, or portions, of the system as the system performance requirements evolve. During the Validation Phase, the PO should monitor the results of the contractor's analyses, trade studies, sizing and timing studies, and modeling efforts. The System Design Review (SDR) should include a presentation of all changes to the System Specification resulting from these Validation Phase studies. This information supports the evaluation of the system design at this stage of development and prevents misunderstandings on the part of the project participants.

By the end of the Validation Phase, the System Specification should be updated to reflect the results of the studies performed and to identify the CIs and CPCIs which were defined. Validation of the updated System Specification should address the same considerations used in validating the initial System Specification. In addition, the PO should address the following new considerations.

- All CIs and CPCIs must be defined.
- All interfaces between the CIs and CPCIs must be identified.
- System engineering trade studies produced during the Validation Phase should focus upon potential risk areas and should demonstrate that Full-Scale Development can proceed within the proven state of the art (i.e., no research or advanced development is required before entering Full-Scale Development). The following considerations are of particular importance to the software:
  - Engineering studies must demonstrate that the software performance requirements can be met within the capacities of the specified computer hardware.
  - All risk software, such as radar processing algorithms for new types of radar equipment, should have been demonstrated, preferably with actual equipment and prototype software or, alternatively, with simulation techniques. (This type of risk analysis should not be confused with top-down design, which is normally conducted during Full-Scale Development.)
  - All timing-critical areas should be carefully examined, individually and as a whole. These include communications and sensor interfaces with specific timing constraints, display response time requirements, and startover/recovery timing requirements.
  - Costs related to timing and capacity requirements should be identified and reviewed. In some cases significant cost savings can be realized by relaxing certain stringent timing requirements.

The PO should be acutely aware of the allocation of functions to CPCIs. The initial functional breakout in the System Specification may not map well into CIs, CPCIs, and operator functions, after hardware/software/human engineering trade studies have been done and the system architecture developed. An attempt to force a CI/CPCI definition consistent with the initial System Specification may result in unduly complex interface requirements. Therefore, consideration should be given, during the Validation Phase, to either revising the System Specification to reflect the allocation of CIs or to developing a clear cross-reference between functions and CIs/CPCIs.

(Page 16 blank)

SECTION 3 - INTEGRATING THE SOFTWARE

This section addresses the activities involved in integrating into the system the qualified CPCIs which were verified during FQT. At this point in the system acquisition cycle, the software has been tested and the individual CPCIs are now ready to be put together and checked out in preparation for System DT&E.

3.1 OBJECTIVES

The PO at this time has had an opportunity to observe the results of FQT and should have a high degree of confidence that each CPCI is functionally correct. Now the contractor must demonstrate that the software performs correctly when assembled into the system in an environment which may differ markedly from that used for CPCI development and test.

3.2 SOFTWARE INTEGRATION CONSIDERATIONS

The factors requiring the PO's consideration during software integration will vary greatly from system to system. They include complexity of the system, the number of external interfaces, the configuration of the software development versus the system integration facilities, and the contractor's approach to software development.

Software integration is normally the responsibility of the contractor. Even in acquisitions which use a mix of contractor and in-house resources for software development, no attempt should be made to split integration responsibilities because of the delays and risks likely to be incurred.

Because a Product Baseline has been established for the CPCIs being integrated, formal change reporting, using Engineering Change Proposals (ECPs), must be followed. Class II ECPs are used to correct errors (e.g., changes which correct deficiencies between the Product and Allocated Baselines) while Class I ECPs are used for those changes which affect both the Product and the Allocated Baseline (see Ref. [13]). If in-house development was done, the personnel and support tools used for development should be used to support integration activities.

Installation and Checkout (I&C) plans should be made CDRL requirements by including the appropriate DID for System DT&E and modifying its contents via a backup sheet (see Ref. [11]). These plans should include a description of all integration activities, schedules, and support requirements. Since the PO may have to provide support in the form of GFE, computer time, display equipment, and communications and support personnel, the submission of an I&C plan should be scheduled [in the Contract Data Requirements List (CDRL)] so that ample time is allowed for the PO to plan and schedule such support. Particular attention should be paid to support requirements which involve other contractors or Government agencies to assure that appropriate agreements or contractual arrangements are made in a timely manner.

Schedule monitoring becomes particularly important at this time. When other agencies are called upon for integration support, the PO must be aware of the impact of schedule changes on both the system under development and the agencies which are preparing to provide support during a particular time period. The PO must be aware that supporting agencies have other commitments, often operational requirements, which may preclude their participation or support during certain periods (e.g., exercises or increased alert situations) and should therefore always keep the supporting agencies advised of planned or possible schedule changes.

The PO must also closely monitor the installation and checkout activities of the system hardware for potential software impact. All ECPs which are approved as a result of hardware installation and checkout must be evaluated for any impact on software. Hardware/software interfaces which vary only slightly, as far as timing or form of response (e.g., timeouts or error returns), may have a large impact on the software. For example, an interface, due to distance, may have to be operated at less than the rate specified. This type of change may require software redesign.

In reviewing and approving I&C plans, the PO should consider the differences between the hardware configuration of the software development facility and that of the test facility. If the software development facility equipment is a subset of the test configuration, for example, differing only in numbers of consoles or display devices, the PO should assure that the integration plan emphasizes the areas which differ between the two facilities, such as timing and capacities. Software that adequately supported a few consoles during an FQT may encounter significant problems when the complete complement of consoles is being driven. On the other hand, if the software was largely developed and verified on a configuration which was markedly different from that of the test facility, integration should include a methodical process of validating each interface prior to attempting any timing or capacity tests. These differences should also be considered in scheduling time for integration.

The PO should also consider the software development approach being taken. One approach is to develop CPCIs and verify their operation in an independent fashion (i.e., each CPCI is developed as a stand-alone entity and testing is accomplished through the use of test tools to generate the inputs and record the outputs of the CPCI). Only after all CPCIs have been verified in this manner should they be integrated into the system. A slower but more thorough approach is to integrate the system software as it is being developed through a series of "builds" or "releases." Each build contains CPCs or modules from one or more CPCIs, with each build adding capabilities not contained in the previous one. The final build comprises the integrated software. In this case FQTs are held at the System DT&E facility in an incremental fashion using qualified portions of the system to drive or provide inputs to the portion under test. There are also development schemes which utilize a combination of these approaches. The degree to which the software was integrated prior to FQT will greatly affect the length and conduct of system integration and checkout.

The PO should track deficiencies uncovered during FQT, especially when certain functions could not be completely tested due to limitations in the developmental facility's hardware configuration. Functional requirements whose qualification has been delayed until the System DT&E environment is available should be stressed during integration. The primary function of integration testing is to assure that the system is ready for System DT&E. All deficiencies uncovered during FQT but not corrected in the developmental facility should be resolved during software integration in the test facility environment. All known problems should be eliminated, if possible, prior to System DT&E.

The PO must also be concerned with external interfaces which are of prime importance during System DT&E. Such interfaces, at this point, have probably been described in the interface specifications contained in paragraph 3.1.5 of the System Specification, but not actually tested. Additionally, the PO should expect inadequacies in the interface requirements. These inadequacies are most often uncovered during integration. Again, the PO must coordinate and schedule some amount of time during integration for the checkout and debugging of these interfaces. This may be particularly difficult if an operational site is used as the System DT&E site and concurrent operations and integration activities are scheduled (e.g., sharing communication links). If uncoordinated links (those where the receiver is not required to acknowledge receipt of data) are involved, the problem can usually be solved by simple bridging of inputs. Where coordination between the sender and receiver (block or message acknowledgement) is required, the problem becomes more complex and may require special arrangements. The PO should be aware of the capabilities and limitations of external interfacing systems so that integration can be properly coordinated and all assumptions regarding the interfaces will be valid.

Software integration is a prelude to System DT&E. System DT&E normally involves a number of agencies and large numbers of personnel. It is, therefore, not cost effective to begin System DT&E until the PO is confident that known deficiencies have been corrected where possible. The final system integration activities should be treated as a dry run of System DT&E. The System DT&E personnel should be trained during the system integration period.

SECTION 4 - THE SOFTWARE ASPECTS OF SYSTEM VALIDATION

This section addresses the software-related activities involved in planning and executing a comprehensive System DT&E program. Although the objective of System DT&E is the formal qualification of the system, there are unique aspects of planning and conduct which are software related and should be so recognized at the very beginning of the system acquisition cycle.

4.1 OBJECTIVES

The objective of System DT&E is to validate the fully developed and integrated system against the requirements contained in the System Specification. At this stage in the system acquisition cycle, all of the CPCIs have been functionally qualified and integrated. During System DT&E, the test effort should present integration problems or situations to the system, function by function. Emphasis should be on the interaction between the various functions, system timing and throughput, priority recognition, and failure mode processing.

4.2 PLANNING FOR SYSTEM VALIDATION

Planning for System DT&E should start at the beginning of the system acquisition cycle. The PO should include validation considerations in the Program Management Plan (PMP), the Test and Evaluation Master Plan (TEMP), the System Specification, and the System DT&E plan. Since these are the principal documents which establish the requirements and resources for System DT&E, they form the basis for all subsequent test activities. They should be responsive to the Test and Evaluation Objectives Annex (TEOA) of the Program Management Directive (PMD).

4.2.1 PMP Considerations

The principal software-related items which should be included in the PMP and which affect System DT&E planning are:

- The identification of software system validation expertise to be allocated to the PO for the management of the test program. The PO's test organization should include personnel who are knowledgeable in the program-specific software from the outset of the program.
- Requirements for simulation capabilities to support System DT&E, if needed for system testing inputs.
- Requirements for a system test facility, if necessary, based on both System DT&E and planned system deployment support requirements (see Ref. [9]).

- A realistic master schedule containing all the major milestones, key events, and critical actions related to software acquisition.

- An identification of required external interfaces to be accommodated by the system.

- A discussion of growth and spare capacity requirements.

- An identification of support required from outside agencies.

Since the PMP is the initial planning document produced by the PO, it forms the basis for all subsequent activities. The inclusion of the above items in the PMP will insure that the PO has the resources to plan and conduct System DT&E and provide a basic understanding of what must be tested.

4.2.2 TEMP Considerations

Since the TEMP identifies responsibility for the various test activities, specifies the time phasing of tests, and delineates test requirements, the PO should assure that it incorporates the following software-related considerations:

- Identification of the specific support and participation expected of each agency.

- Delineation of the responsibilities for providing test facilities, personnel, and training.

- Schedules for system integration and System DT&E which are consistent with the schedules for individual CIs and include sufficient time for resolution of problems.

- A clearly specified test environment for System DT&E. This may include special test adaptation or the use of simulation to support testing.

- Specification of instrumentation requirements. The provision or lack of hardware measuring devices may impact the amount of software required to record or measure system performance parameters.

- Specification of the required documentation (e.g., positional handbooks, users manuals).

A comprehensive TEMP will provide PO software personnel with (1) the basis for planning those activities which must be supported and (2) identification of the software capabilities needed to support System DT&E.

4.2.3 System Specification Considerations

The System Specification must include requirements for software support for System DT&E. The functional areas most often impacted to support System DT&E are simulation, data recording, and data reduction. The requirements delineated in the System Specification should be reviewed by the SD to assure adequate coverage of both operational and support requirements so that a cost effective system validation program can be established.

Simulation capabilities may or may not be an operational requirement but typically some simulation will be required to test the software during development. The question of how System DT&E inputs are to be provided should be addressed in the TEMP in sufficient detail so that the System Specification can include simulation requirements for the conduct of System DT&E if live inputs are not available. In most cases, even when live inputs are available, simulation is required for maximum load testing, especially when the system must accommodate a wartime threat scenario. The inclusion of simulation requirements in the System Specification assures that sufficient capability will exist to support System DT&E.

Similarly, recording, and data reduction capabilities may or may not be operational requirements, but they are almost always required to some degree for support of all levels of testing. A comprehensive test program will include these requirements in the QA section of the System Specification in a form which is compatible with the TEMP.

If the simulation, recording, and data reduction requirements to support System DT&E are not included in the System Specification, the PO will have to face the problem of adding them as new requirements by processing ECPs. If an attempt is made to use unqualified software development tools for System DT&E, the lack of documentation and the possibility that the unqualified tools are inadequate, are likely to create problems. Since some form of these capabilities will undoubtedly be required for operational support, a planned approach which includes acquisition of qualified tools (e.g., qualified prior to their use in System DT&E) is usually the most cost effective.

The adequacy of Section 4, Quality Assurance, of the System Specification should be the second area of concern in planning for a successful System DT&E.

QA provisions in Section 4 should correspond directly to specific requirements in Section 3 of the System Specification and should specify their validation by use of a specific method during a specific phase of testing. These methods normally include:

- Inspection. Validation by visual examination of the item, reviewing descriptive documentation, and comparing the appropriate characteristics with a predetermined standard to determine conformance to requirements without the use of special laboratory equipment or procedures.

- Analysis. Validation by technical, mathematical, or analytical evaluation using mathematical models, algorithms, equations, charts, graphs, circuit diagrams, or data reduction, for representative data.

- Demonstration. Validation of operation, movement, or adjustment of the item under a specific condition to perform the design function without recording quantitative data, except for check sheets. The item may be instrumented and quantitative limits of performance monitored but actual data is not required to be recorded.

- Test. Validation by systematically exercising the applicable item under all appropriate conditions with instrumentation and collection, analysis, and evaluation of quantitative data.

The PO should review the phase and method carefully to assure that the proper method is selected and the proper phase of testing is specified (i.e., CPT&E, Subsystem DT&E, System DT&E).

During System DT&E, analysis, demonstration, and test are all appropriate methods for software validation. The method selected should conform to the manner in which the requirement is stated in section 3 of the System Specification. A review of sections 3 and 4 for compatibility may identify an inadequate requirement statement in section 3, if it is not clear how the requirements should be validated.

System DT&E should require a minimum of redundancy with previous phases of testing, e.g., CPCI DT&E (see Ref. [12]), and should be directed primarily toward those requirements which involve the entire system, e.g., response time, throughput, failure modes, recovery, operator interaction, and interaction between CIs.

Section 4 should also contain specific qualification criteria. The System Specification should identify:

- What should be tested in System DT&E.

- How much testing is required.

- The test environment.

- The acceptance criteria.

- The test facilities and support tools required for Deployment.
- Test responsibilities.

The PO should, after assuring that the PMP, TEMP, and System Specification consistently define the approach to System DT&E, keep these documents current as the system acquisition cycle proceeds. They should be used as living, working documents and updated as changes occur which affect methodology, responsibilities, or requirements.

4.2.4 System DT&E Plan Considerations

Although System DT&E is the PO's responsibility, the contractor usually provides System DT&E Plan/Procedures inputs. The PO should review these inputs to ensure that:

- Any requirements for CI or CPCI qualification will be completed before System DT&E begins.
- The plan presents an overall integrated outline of the total System DT&E program.
- The plan has been coordinated with all participating agencies.
- The planned test environment is as realistic and complete as possible. Live inputs are used whenever feasible.
- Tests planned for System DT&E are not duplicates of previous tests used for CI qualification.
- Responsibilities for test conduct and participation are clearly delineated.
- Test schedules are clearly presented and are consistent with the expected completion of system integration.
- All facilities, equipment, personnel, and support software requirements are included.
- A procedure exists for every planned test.
- Specific data collection and analysis requirements are stated.
- Problem reporting, isolation, statusing, and correction procedures are included.
- Step-by-step guidance on the conduct of each test is included in each procedure.

- Plans and procedures include a comprehensive evaluation of the integrated CPCIs with emphasis on risk areas.

- Compatibility and performance of all support software will be evaluated within the System DT&E environment.

Review of System DT&E Plans/Procedures should also include considerations regarding their continued validation/use throughout the system life cycle. In most cases each test should be functionally oriented (i.e., weapons, surveillance). The procedures should be written in script form containing a planned sequence of events intended to validate the entire function within the system environment. As changes (ECPs) to the system are introduced during Deployment, the System DT&E Plans/Procedures should be continually updated and used to ensure their continued value throughout the system life cycle.

4.3 MONITORING ACTIVITIES

During the Validation and Full-Scale Development Phase, the PO is usually in a monitoring role; reviewing and approving specifications and System DT&E plans and procedures, attending reviews, witnessing qualification tests, monitoring schedules, and coordinating activities. During this period, the PO should be concerned with continued planning for System DT&E. The PO should:

- Continue to review the System DT&E Plan and procedures for adherence to test requirements as described by the TEMP and System Specification. This review should include System DT&E facility requirements, test support software requirements, and test instrumentation.

- Assure that test scenarios or test cases are either developed by the contractor or provided to him, that they are consistent with the mission requirements, and that they have been properly coordinated with Government agencies.

- Review CPCI DT&E plans for overlap with System DT&E and for items which, because of development facility limitations, are deferred until System DT&E. The objective is to reduce redundant testing and assure that testing is done in the most economical and realistic environment.

- Assure that critical functions are tested early enough so that problems encountered can be rectified without costly schedule impacts.

- Monitor all I&C activities. Particular attention should be paid to interface testing during I&C; inadequate interface testing at this point can cause major delays in System DT&E.

- Assure that System DT&E truly stresses the entire system in a manner closely approximating the operational environment and is not fragmented to the point where results are meaningless. For example, timing and throughput testing, which do not include proper simulation of inputs, operator actions, and outputs, can yield false results.

- Monitor training plans to assure that System DT&E personnel have the proper training and that documentation is available for their use (e.g., operators guides, positional handbooks, and user guides).

- Review System DT&E procedures to insure that the data collection, reduction, and analysis techniques are valid and that only qualified software will be used for input generation and for recording and data reduction. If special software test tools are to be used, the PO should establish procedures for their qualification.

- Review all ECPs for impact on System DT&E documentation and ensure that updates are made as required.

- Assure that adequate configuration management procedures are available for the control and retention of System DT&E materials. These materials should only be changed via controlled procedures.

- Assure that required support from external agencies will be available and that schedule changes are properly coordinated.

- Assure that site-unique adaptation data is documented and available for the System DT&E environment (e.g., positions of both live and simulated radars).

4.4 SYSTEM DT&E CONDUCT

During conduct of System DT&E, PO software personnel should be part of the system test team and, whenever possible, should be the same personnel as those participating in the Functional Configuration Audits (FCAs) of the CPCIs to assure continuity of knowledge from the CPCI DT&E. They should:

- Not allow System DT&E to continue until all CIs and CPCIs have been qualified.

- Observe or participate in the test conduct.

- Participate in or review the analysis of test results.

- Review analysis of system problems encountered during test conduct for potential software errors.

- Assure that all software changes made to correct problems were properly tested prior to conduct of System DT&E. This may require the review of special tests to verify proper system operation.

- Advise the Test Director on all software matters, alternative work-arounds if required, and on tentative solutions to system design problems.

PO software personnel should be aware that, even with the best of planning, System DT&E seldom goes smoothly (e.g., external interfaces are not exactly as anticipated, timing problems arise which went undetected during previous phases, operators do not always follow scripts and procedures, and an operational environment presents unforeseen problems). PO software personnel are often in the best position, due to their previous activities, to assist the Test Director in developing work-arounds to these problems. Their experience, gained in the monitoring of previous testing, should be used to assist operations, suggest "quick fixes" to interface and timing problems, and assess the criticality of problems. Typically, a software solution may be the quickest method of temporarily (or permanently) solving a problem which is delaying testing and incurring heavy costs; PO software personnel should not hesitate to recommend such solutions.

SECTION 5 - PLANNING FOR CERTIFICATION

Certification starts the Deployment Phase and indicates the operational suitability of the system. While certification is the responsibility of the using command, the PO is involved in planning and preparing the Operational Test and Evaluation (OT&E) which concludes with certification. Further, some of the PO personnel involved in the development of test and support plans may participate in development of turnover and transfer agreements to assure continuity of liaison and coordination between the operating and supporting commands. Just as the operating command may support System DT&E with liaison personnel, facilities, test data, and general assistance in evaluating test results, the PO may support OT&E.

5.1 PLANS

Joint involvement of the implementing, operating, and supporting commands in the planning for OT&E is inherent in all those plans requiring coordinated command participation and concurrence. These include:

- Test and Evaluation Objectives Annex (TEOA)
- Test and Evaluation Master Plan (TEMP)
- Computer Resources Integrated Support Plan (CRISP)
- Turnover Agreements
- Program Management Responsibility Transfer (PMRT) Agreements
- Operational/Support Configuration Management Procedures (O/S CMP)

The TEMP, the CRISP, PMRT Agreements, and Turnover Agreements establish responsibilities, schedule activities, and commit resources to system acquisition. Furthermore, they lay the groundwork for test and evaluation plans at all levels (validation, certification, and verification).

In the case of programs that are directed by Hq. USAF, the Air Force Test and Evaluation Center (AFTEC) has the major responsibility for providing the test and evaluation portions of Decision Coordinating Papers (DCPs) and Program Management Directives (PMDs), including the TEOA. Such directives are issued both to initiate the program and to govern it during acquisition. AFTEC will request test and evaluation input from both the operating and implementing commands.

The military environment is subject to reorganizations, changes to policy and procedures, and even to shifts in the hostile threat. Many of these changes may result in ECPs to the system or cancellation of a system due to changing needs. Because of the time lapse between ROC and certification it is inevitable that operational SOPs will change. Even major operational requirements may change and the system delivered for certification may no longer be compatible with the operational environment. A major purpose of OT&E is for the using command to assure compatibility between the delivered system and current SOPs. For most systems, a large number of ECPs may be expected immediately after delivery to clear up such minor misconceptions and incompatibilities. These incompatibilities should be minimized through close liaison with the operating command.

The TEMP, an overall test and evaluation plan, identifies and integrates the efforts and schedules for all tests and evaluations performed in connection with the new system. In addition to the tests for CPCI qualification (see Ref. [12]), the TEMP may also identify Initial Operational Test and Evaluation (IOT&E) system components prior to the production decision (see Ref. [1]). In the TEMP, the implementing, operating, and supporting commands document support agreements and joint enterprises. The operating command may agree to supply operational facilities, personnel, and data for System DT&E. The implementing command may agree to supply test cases and personnel for OT&E. In the case of joint testing, where IOT&E may be combined with System DT&E, the roles and responsibilities of both commands are delineated. On major programs AFTEC too will be intimately involved for both initial and follow-on OT&E for joint tests. Further, AFTEC support requirements for OT&E must be considered in the TEMP and CRISP and priorities and budgets established.

The CRISP is especially important for certification planning since it outlines the computer resources support required both before and after the transfer of program management responsibility. It identifies the configuration management practices, the documentation, the personnel, and the hardware and software required to support the operation of the system. In addition, it outlines testing, transfer, and turnover procedures. The CRISP also identifies responsibilities for maintaining the integrity of the system, including interface control, baseline document maintenance, control and accounting of computer and storage usage, and processing priorities. The implementing command, with the support of the Computer Resource Working Group (CRWG), is responsible for generating the CRISP and setting up the procedures to be used before and after transfer, with the supporting and operating commands taking an active role in its preparation. The CRISP ensures the adequacy and continuity of computer resource support and maintenance after the transfer of program management responsibility (see Refs. [8&9]).

Both the turnover and transfer agreements may include requirements for the implementing command to continue developmental support in addition to the test and evaluation commitments of the TEMP. A system may be accepted provisionally for OT&E while still leaving the PO responsible for the implementation of changes (ECPs), and the removal of system deficiencies.

Many systems are developed and delivered in an incremental fashion. This approach may be desirable and for any of the following reasons:

- Achieves an operating capability earlier than the complete system development schedule would permit.

- Reduces risk due to system cost, production difficulty, or advanced technology.

- Provides a prudent approach to system design since its iterative features reduce the risk that a system will not perform satisfactorily when operational.

Whenever incremental development is adopted, an extended period of successive developments and deliveries occurs. This results in the TEMP and the CRISP being revised to some degree for each version of the system. A joint operating/supporting/implementing command configuration management program should be established to maintain accounts for all versions of the system and to efficiently process software problem reports resulting from both operational experience and System DT&E.

5.2 TURNOVER AND TRANSFER

Turnover and transfer agreements must be formulated early in the acquisition cycle since there are budgetary assignments to be made, responsibility agreements to be concluded, and support items to be evaluated. At least some of the personnel* (see paragraph 6-10 of Ref. [3]) that developed the original TEMP and the CRISP should be involved in development of the turnover and transfer agreements to assure continuity of liaison and coordination with supporting and operating commands. The assigned personnel should have relatively long-term assignments to allow the adequate preparation of a variety of joint plans which culminate in the observation and evaluation of system tests and their results.

The groups appointed to prepare the TEMP, the CRISP, and the turnover and transfer agreements should be composed of representatives of each of the implementing, supporting, and operating commands. In the case of a multi-service system, similar groups should be appointed by each responsible service. At the end of validation or at any other agreed upon time, turnover and transfer should be accomplished in accordance with the agreements between the commands. In each case (the turnover agreement and the transition memorandum), a version description should be included, listing all the system elements (and specifically identifying all computer resource elements) and detailing all the known deficiencies and exceptions still to be corrected and delivered (see Section III of Ref. [11] and paragraph 5.4 of Ref. [13]). All significant conditions and residual tasks with schedules for their completion and/or resolution should also be included. The final document must be countersigned by all participating commands.

Once the transfer of program management responsibility has occurred, the implementing command no longer has system responsibility. Since further development must treat the system as Government Furnished Property (GFP), new versions and significant modifications and extensions need joint-management attention.

*The same people may also participate in preparation of the O/S CMP, which provides details on configuration management agreements in the CRISP.

The importance of these events to program planning, budgeting, and scheduling cannot be over-stressed. Once the transition has occurred, funding for additional procurement must be budgeted by the supporting command. Turnover and transfer plans and agreements are significant inputs to command plans and budgets. They must be available well in advance of their need so that proper preparations can be arranged.

In preparing for system turnover, the PO must assure that the following set of conditions and principles (see Refs. [2, 4, 5, & 6]) have been met:

- All software is of a uniform configuration. The PO should minimize deliveries with malfunctions and unaccomplished modifications. Outstanding ECPs should be incorporated before turnover, to the extent practicable.

- Manpower requirements (skills and quantity) have been provided for through the CRISP and the O/S CMP. If any portion of the system is to be contractor maintained or operated after turnover, identify the affected system or subsystem and the period and extent of contractor maintenance and operation.

- Support and training has been adequately planned and prepared; including:

  - Compatibility of the software maintenance concept, support equipment, and expected maintenance workload.

  - Qualified test support software, interface devices, and automated test equipment.

  - Application of configuration control procedures, including change analysis and change implementation, equally to support equipment, computer programs, and mission equipment.

  - Adequate calibration and technical data for maintenance of support and training equipment and computer programs.

  - Adequate provision of simulation and software support equipment.

- Technical publications and computer resource documentation are accurate and available.

- Facility requirements are identified with appropriate lead time (2 years normally).

- Budgetary needs are identified.

- Information on the operational characteristics of the system has been provided early enough to permit operating procedures and standards to be prepared.

- The transition from Contract Engineering Technical Services (CETS) to blue suit maintenance has been adequately prepared, if required.

- Control and distribution procedures for software changes have been established.

Transfer of program management responsibilities normally occurs during the Production Phase. It may occur at any logical point when the following criteria are met:

- The Product Baseline for each CI/CPCI has been firmly established.

- Product qualification has been established (i.e., the product has been accepted and the Form DD250 has been signed).

- Specified design and performance requirements have been successfully demonstrated by System DT&E (see Ref. [1]).

- All required updating changes (ECPs) have been identified and approved.

- Mutual agreement has been reached that adequate engineering and technical order data are available for operation, configuration control and accounting, maintenance, and other necessary logistics support requirements.

- The remaining changes are documented as deferred items or tasks of the turnover until completed by the implementing command.

5.3 OT&E SUPPORT ACTIVITIES

Besides including and discharging IOT&E objectives in System DT&E, there are several specific ways in which the PO may support OT&E, including:

- Training

- Test-case generation

- Operational-procedures development

Although user training is normally the responsibility of the using command, in conjunction with Air Training Command, it is the developers who, because of their knowledge of the system, are in the best position to train user personnel for OT&E. While there is usually sufficient time to train user personnel for ongoing operations, getting ready for OT&E requires extensive preparations with little lead time. Further, operator training is best done hands-on and the system is seldom available much in advance of OT&E. To facilitate the training of user personnel for OT&E, the personnel used in System DT&E can often be used to form a cadre for OT&E. In addition, if the validation effort maintains a separate test facility for System DT&E the test facility may also be used for system familiarization (if not full-scale training) before OT&E. It also helps to prepare familiarization and indoctrination courses and briefings to acquaint user personnel with the system and to prepare them for acceptance of the new mode of operation. In fact, it is often desirable to contract for course preparation and training services to train operational and maintenance personnel so that they may assume the operational training load.

The delivery of planned tests and test cases to be used in OT&E is also a valuable support service that can be procured. It is in the interest of both development and support commands that simulated and actual test inputs be as similar as possible. This similarity provides test results which are comparable and supports an early understanding of system operations. It also avoids some redundancy in the test process.

The PO can also be of material assistance in the development and documentation of operational procedures, an activity unique to the operating command, just as the creation of users manuals, console guides, and positional handbooks is a developmental function that can profit by the assistance of operational personnel. Similarly, the revision of procedures that reflect the new system operation can profit from the review of developmental personnel.

SECTION 6 - MANAGEMENT OF SYSTEMS UNDER TEST

The configuration management practices that are applied to CPCI development and test are basically the same as those which should be applied during System DT&E and OT&E, including:

- Maintenance procedures for test documentation.
- Protecting the integrity of products being tested and evaluated.
- Accounting for test, product, and ECP status.
- Procedures for reporting, evaluating, and correcting errors.

6.1 MAINTENANCE OF TEST DOCUMENTATION

The maintenance of test plans and test procedures for System DT&E is often a problem because of the length of time that elapses between the issuance of documents and their use. PO attention is usually focused upon product development and contractor activities rather than upon ensuring up-to-date documentation to support validation and certification activities. There is, therefore, a tendency to neglect the maintenance of these documents. Updating after a lapse of months is hindered by the writer's tendency to forget details and the confusion of changes to changes. Good configuration management practices call for the maintenance of all documentation affected by a change as soon as practicable.

To ensure maximum traceability, test documentation should receive specific identifiers, change pages should be issued to update the documents, Specification Change Notices (SCNs) should be issued to transmit change pages to all affected documents, and indexes of effective pages should be kept so that each document can be checked for currency before use.

System DT&E documentation should be reviewed in the same manner as CI qualification test documentation and Product (Part II) Specifications. All changes to the System Specification should be reviewed to determine whether changes to the System DT&E plan or procedures are required.

6.2 PROGRAM LIBRARIES

When a qualified CPCI is delivered, its integrity is guaranteed by the contractor, that is, he delivers a clean deck with all changes incorporated and errors corrected. The Product (Part II) Specifications, user's manuals, and other documentation have also been checked by the PO at the PCA. In short, the PO is accepting delivery and responsibility for a checked-out, qualified product. Any change made to it after this point is an Air Force responsibility. It is now Air Force property and its integrity is no longer a contractor responsibility.

If the contractor was acting in accord with the latest recommended practices, the qualified CPCI was kept in a protected version of a Program Production Library (PPL)[1]. Any modifications to be made to a CPCI in this library are first made and tested in a test library version and only fully tested and qualified CPCIs are placed in the system master version. Similar procedures, whether automated or manually performed, should be adopted for the System DT&E program library. If any changes or corrections are made to the programs, a test library should be created and all modifications thoroughly checked before substitution into the master. It is good practice to maintain several backup masters so that the System DT&E effort can go back to a version of known test status if a new version proves faulty.

6.3 TEST STATUS REPORTS

System DT&E like any other test activity is a period of high activity, prone to confusion and uncertainty about current test status. System DT&E is often more prone to confusion than CPCI DT&E since many combinations and interactions of CIs are tested. Test status may be uncertain since, if a test has failed and corrections or modifications are made, then the validity of previously passed tests may be questionable. Because unforeseen problems are often encountered, daily reassessments of work remaining should be accomplished. If one string of tests must be halted because of a problem area, alternate paths may be taken. Exact status (of tests, functions, interfaces, and known problems) kept on a daily basis is mandatory to support System DT&E.

Status accounting is also required to keep track of suspected and reported discrepancies, the incorporation of changes into the system under test, and to record the fact that each change has been tested before continuing System DT&E. Status reports should be issued on a frequent basis during System DT&E and the test director must be prepared to provide status information on a demand basis.

---

[1] See Appendix A of the Verification guidebook for a description of the PPL.

6.4 SOFTWARE PROBLEM REPORTING AND CORRECTION

After CPCI acceptance, all newly encountered problems should be officially reported and controlled by the PO. A form such as a System Problem Report (SPR) or Discrepancy Report Form (DRF) can be used. An official review board, normally a Configuration Control Board (CCB) or a subgroup thereof, keeps a log of the reported errors, gathers diagnostic analyses and recommendations for correction, monitors actual modifications in the form of ECPs, and keeps status accounts of ECPs. Errors discovered during System DT&E and OT&E differ only in who is responsible for program management. That is, the implementing command or the using command owns the software and the contractor is no longer responsible for its integrity unless he is on a maintenance contract.

There are a number of issues associated with the processing of software problem reports, including:

- Who is responsible for reporting problems?
- Who shall determine the disposition of the problems?
- Who shall diagnose the difficulty and recommend solutions?
- Who shall create and install corrections?
- How shall corrections be controlled?

6.4.1 Reporting Problems

Theoretically, during System DT&E and OT&E, system test and user personnel are responsible for the system. However quite often there are numerous contractor personnel on hand (under latent defect clauses, maintenance contracts, or system integration contracts) observing the tests and performing maintenance on the system. During tests or during diagnostic and checkout runs, these persons too may note potential problems. In general, if everyone associated with a project is permitted to file problem reports, a great many invalid reports appear, placing some extra burden on the CCB and the accounting system. It is best if errors can be reported informally to a qualified control technician who is charged with evaluating reports, gathering pertinent data and filtering the reports. The control technician must understand the System Specification and system user documentation. He may work for the PO or for a contractor but should report to the Test Director. The prescreening ensures that with minor exceptions, valid problems are reported and the reports are accompanied with at least a modicum of supporting information so that the problems can be recreated.

6.4.2 Problem Disposition

The formality of the decision process by which the disposition of problem reports is determined can create some difficulties. If supplier personnel are on maintenance contract and readily available, problems can be turned over to them directly by the CCB to be fixed. Such a procedure has the advantages of speed and responsiveness. However, formal processing of problem reports can be a time-consuming process. The CCB (or alternate) may not meet every day, formal analysis reports require time to prepare and review, and significant interruptions to testing may result. Formal procedures do protect the integrity of the system and prevent problems being lost or forgotten. It is desirable for the Test Director to assign a Problem Czar who can quickly dispose of problems on a day-to-day basis, but who is constrained to pass significant problems (those impacting several CIs costing appreciably in time, money and effort to fix, or which would require a redesign to correct) on to a more comprehensive configuration control agency. The decision maker needs to be backed up by an efficient problem accounting system and should be directed to actively pursue solutions to all outstanding problem reports. Further, the CCB should review all reported and outstanding problems at least once a week, during System DT&E, to determine where the system stands and provide a check on the Problem Czar's activities.

6.4.3 Responsibility for Diagnosis

The PO Test Director is responsible for System DT&E. He can assign responsibility for problem diagnosis to Air Force or contractor personnel, depending on the resources available to him. The solutions of problems are often not immediately obvious. Diagnostic tests must be run, including trying to reproduce the effects originally noted. If maintenance contracts have been let, system or software engineering personnel may be on hand to diagnose problems. If not, the test team must either perform the analysis or transmit the problem report to the supplier. Sometimes the equipment configuration at the operational site is more austere than at the production facility and is incapable of properly supporting diagnostic efforts. In such cases, analysis and correction must be done away from the test site. Experts should be available from the suppliers both to assist in the conduct of tests and to effect emergency repairs.

6.4.4 Responsibility for Correction

If at all possible, the development contractor should be responsible for correcting the software. Undoubtedly, adequately trained software maintenance personnel may, with time, do as well, but during System DT&E the most knowledgeable people should be used. Further, if the software has been guaranteed or warranted in any way, the warrant is probably invalidated if anyone else makes modifications. However, since close control must be exercised over the software configuration, test personnel should review, test, and accept all corrections before the modifed software is incorporated for further System DT&E.

6.4.5 Correction Control

It is very important to the evaluation of test results that accurate records be kept of reported software problems. Problem reports should be entered into the configuration accounting system in the same way and receive the same processing as ECPs. That is, both are essentially requests for changes to the software and should receive similar consideration. Identifying numbers should be assigned and exact status kept. SPRs should be submitted to a control point (or at least a copy thereof), logged in , and distributed to interested parties; those who are to determine their disposition and those whose product or work is affected.

Analyses are conducted to diagnose the cause of each error and to derive solutions, as well as to make recommendations to the configuration controller for disposition. The control authority may:

- Reject the SPR as invalid.
- Approve its immediate correction.
- Defer correction to a later date on grounds that the problem is trivial (does not seriously impact performance) or that correction would be too costly and time-consuming to accomplish immediately.

If the correction is approved or deferred, an estimate of the time and cost of correction should be made and a tentative schedule set. If no maintenance contract has been let and the corrections cannot be made by available maintenance personnel, an ECP may have to be negotiated. Each action in the life of the SPR should result in a change of status in the SPR accounts. Keeping track of problem status and preparing agenda, amassing change packages, and issuing CCB actions is normally a full time job.

APPENDIX A - GLOSSARY

This appendix consists of (1) definitions of major terms used throughout this guidebook and (2) acronyms and abbreviations used herein.

DEFINITIONS

Certification. As used in this guidebook, refers to the using command's agreement, at the conclusion of OT&E, that the acquired system satisfies its intended operational mission.

Computer Program Component (CPC). A functionally or logically distinct part of a computer program distinguished for purposes of convenience in designing and specifying a complex computer program as an assembly of subordinate elements (MIL-STD-483).

Computer Program Configuration Item (CPCI). A computer programming end product whose development and subsequent modification is subject to configuration management .

Computer Programming Test and Evaluation (CPT&E). Tests conducted prior to and in parallel with preliminary or formal qualification tests. These tests are oriented primarily to support the contractor's design and development process (AFSCM/AFLCM 310-1).

Conceptual Phase. The initial period when the technical, military, and economic bases for acquisition programs are established through comprehensive studies and experimental hardware/computer program development and evaluation. The outputs are alternative concepts and their characteristics, e.g., established operational, schedule, procurement, costs, and support parameters (DODD 5000.1/AFR 800-2). The major definition document resulting from this phase is the initial system specification (AFR 800-14, Vol. II).

Configuration Item (CI). An aggregation of hardware/computer programs or any of its discrete portions, which satisfies an end-use function and is designated by the Government for configuration management. CIs may vary widely in complexity, size, and type, from an aircraft, electronic, or ship system to a test meter or round of ammunition (abbreviated, from AFR 65-3).

Critical Design Review (Computer Program). A formal technical review of the design as depicted by the specification and flow diagrams, sufficiently detailed to enable the programmer to code, compile, and debug a computer program, to assure that design requirements have been met before coding begins.

Deployment (Operational) Phase. The period beginning with the user's acceptance of the first operational unit and extending until the system is phased out of the inventory. It overlaps the production phase (DODD 5000.1/AFR 800-2).

Development Specification. A document which specifies the total functional performance requirements for each CPCI. This specification represents a comprehensive and definitive statement of the performance, design, and test requirements to be met by the computer program. Equivalent to "Part I CPCI specification" or "Type B5 specification."

Development Test and Evaluation (DT&E). Test and evaluation conducted by the implementing command and its contractors to demonstrate that the design and development process is complete and that the system will meet specifications.

Engineering Change Proposal (ECP). A term which includes both a proposed engineering change and the documentation by which the change is described and suggested (MIL-STD-480).

Formal Qualification Tests (FQT). Formal tests oriented toward testing of the integrated CPCI, normally using operationally configured equipment at the Category II site prior to the beginning of Category II testing. This testing will emphasize those aspects of the CI performance which were not verified by preliminary tests [MIL-STD 483(USAF)].

Full-Scale Development Phase. The period when the system/equipment and the principal items necessary for its support are designed, fabricated, tested, and evaluated. The intended output is, as a minimum, a preproduction system which closely approximates the final product, the documentation necessary to enter the Production Phase, and the test results which demonstrate that the production product will meet stated requirements (DOD 5000.1/AFR 800-2).

Functional Configuration Audit (FCA). A formal audit to validate that the development of a configuration item (CI) has been completed satisfactorily and that the CI has achieved the performance and functional characteristics specified in the functional or allocated configuration identification.

Implementing Command. The command charged with primary responsibility for developing and acquiring the system, including its equipment and computer programs.

Operating Command. The command charged with primary responsibility for operational employment of a system, subsystem, or items of equipment and computer programs.

Operational Test and Evaluation (OT&E). Test and evaluation of operational configuration items to assess the system operational effectiveness and suitability in a deployment configuration (AFR 800-14, Vol. II).

Physical Configuration Audit (PCA). The formal examination of the "as built" configuration of a unit of a CI against its technical documentation in order to establish the CI's initial product configuration identification (MIL-STD-480).

Preliminary Design Review (PDR). A formal review of the preliminary design of a system functional area or of a configuration item to establish system compatibility of the design, identify specific engineering documentation, and define physical and functional interface relationships.

Preliminary Qualification Tests (PQT). Formal tests oriented primarily toward verifying portions of the CPCI prior to integrated testing/formal qualification tests of the complete CPCI. These tests will typically be conducted at the contractor's design and development facilities [MIL-STD 483 (USAF)].

Production Phase. The period from production approval until the last system/equipment is delivered and accepted. The objective is to efficiently produce and deliver effective and supportable systems to the operating units. It includes the production and deployment of all principal and support equipment (DODD 5000.1/AFR 800-2).

Program Management Responsibility Turnover (PMRT). (See Transfer)

Product Specification. A document or series of documents which contain the detailed technical description of the CPCI as designed and coded. It is a complete description of all routines, limits, timing, flow, and data base characteristics of the computer program, including listings of the coded instructions. Equivalent to "Part II CPCI specification" or Type C5 specification".

Qualification. Verification by means of tests and other suitable methods that a newly-developed item meets the requirements of its development (Type B) specification.

Supporting Command. The command charged with primary responsibility for program management in the Deployment Phase, including logistics, engineering, and procurements.

System Design Review (SDR). The SDR is conducted to evaluate the optimization, correlation, completeness, and risks associated with the allocated technical requirements.

System Requirements Review (SRR). The SRR is a system engineering review to ascertain the adequacy of the contractor's efforts in defining system requirements. It will be conducted when a significant portion of the system functional requirements has been established.

System Specification. A document which states all the necessary system-level technical and mission requirements in terms of performance, allocates requirements to functional areas (or configuration items), defines the interfaces between or among the functional areas (or configuration items), and includes the quality assurance provisions to assure the achievement of all requirements.

Test & Evaluation Master Plan (TEMP). The TEMP is an overall plan which identifies and integrates the efforts and schedules of all test and checkout activities to be accomplished in the system development program.

Transfer. Refers to Program Management Responsibility Transfer (PMRT). The transfer of program management responsibility for a system (by series), or equipment (by designation), from the implementing command to the supporting command. PMRT includes transfer of engineering responsibility (AFR 800-4).

Turnover. That point in time when the operating command formally accepts responsibility and accountability from the implementing command for the operation and organizational maintenance of the system or equipment acquired (AFR 800-19).

Validation. As used in this guidebook, comprises those evaluation, integration, and test activities carried out at the system level to assure that the finally developed system satisfies the requirements of the System Specification.

Validation Phase. The overall objective of the Validation Phase is to determine whether to proceed with full-scale development. The ultimate goal of the Validation Phase, where development is to be performed by a contractor, is to establish firm and realistic performance specifications (Allocated Baseline), which meet the operational and support requirements.

Verification. As used in this guidebook, the iterative process of determining whether the product of selected steps of the CPCI-development process fulfills the requirements levied by the previous step.

ACRONYMS AND ABBREVIATIONS

AFLC	Air Force Logistics Command
AFR	Air Force Regulation
AFSC	Air Force Systems Command
AFTEC	Air Force Test and Evaluation Center
C^3	Command, Control, and Communications
CDR	Critical Design Review
CDRL	Contract Data Requirements List
CETS	Contract Engineering Technical Services
CI	Configuration Item
CPC	Computer Program Component
CPCI	Computer Program Configuration Item
CPT&E	Computer Program Test and Evaluation
CRISP	Computer Resources Integrated Support Plan
CRWG	Computer Resources Working Group
DCP	Decision Coordinating Paper
DoD	Department of Defense
DSARC	Defense System Acquisition Review Council
DT&E	Development Test and Evaluation
ECP	Engineering Change Proposal
ESD	Electronic Systems Division
FCA	Functional Configuration Audit
FQT	Formal Qualification Test
GFE	Government Furnished Equipment
GFP	Government Furnished Property
HOL	Higher Order Language
I&C	Installation and Checkout
IOT&E	Initial Operational Test and Evaluation
MCI	Computer Systems Engineering Directorate
O/S CMP	Operational/Support Configuration Management Procedures
OT&E	Operational Test and Evaluation

PCA	Physical Configuration Audit
PDR	Preliminary Design Review
PMD	Program Management Directive
PMP	Program Management Plan
PMRT	Program Management Responsibility Transfer
PO	Program Office
PQT	Preliminary Qualification Test
QA	Quality Assurance
ROC	Required Operational Capability
RSSs	Regulations, Specifications, and Standards
SDR	System Design Review
SRR	System Requirements Review
TBD	To Be Defined
TEMP	Test and Evaluation Master Plan
TEOA	Test and Evaluation Objectives Annex

APPENDIX B - BIBLIOGRAPHY

AIR FORCE AND SUBORDINATE COMMAND DOCUMENTS

AFR 80-14; "Test and Evaluation;" USAF; 19 July 1976 and AFSC Supplement 1; 16 June 1975.

AFR 800-4; "System/Equipment Turnover and Management Transition;" 19 November 1971.

AFR 800-14; "Acquisition Management;" USAF:

- Volume I - Management of Computer Resources in Systems; 12 September 1975.
- Volume II - Acquisition and Support Procedures for Computer Resources in Systems; 26 September 1975.

AFR 800-19; "System or Equipment Turnover;" USAF; 27 May 1975.

AFSCR/AFLCR 57-4; "Management of Retrofit Changes During Acquistition;" USAF (AFSC); 20 October 1970.

AFSCR/AFLCR 80-16; "Qualification of USAF Equipment;" USAF (AFSC); 13 November 1968.

AFSCR/AFLCR 80-17; "Air Force Engineering Responsibility for Systems and Equipment;" USAF (AFSC) 10 May 1973. (ESD Supplement 30 October 1973).

AFSCR/AFLCR 800-7; "Transition Planning and Agreements;" USAF (AFSC); 31 January 1973.

AFSCP 800-3; "A Guide to Program Management;" USAF (AFSC); 14 May 1971.

AFSC DH 1-3; "Personnel Subsystem;" AFSC Design Handbook.

GENERAL REFERENCES

"A Definitional Framework;" Hertzel, W. C.; Program Test Methods; Hetzel, W. C. (Ed); Prentice-Hall, Inc.; Englewood Cliffs, N. J.; 1973.

"An Overview of Bugs;" Schwartz, J. T.; Debugging Techniques in Large Systems; Rustin, R. (Ed.); Prentice-Hall, Inc.; Englewood Cliffs, N. J.: 1971

"A Perspective on System Performance Evaluation;" Drummon, M. E.; IBM System Journal, No. 4; 1969.

"Debugging Under Simulation;" Supnik, R. M.; Debugging Techniques in Large Systems; Rustin, R. (Ed.); Prentice-Hall, Inc.; Englewood Cliffs, N. J.; 1971.

"Developing and Testing a Large Programming System, OS/360 Time Sharing Option;" Scherr, A. L.; Program Test Methods; Hetzel, W. (Ed.); Prentice-Hall; Englewood Cliffs, N. J.; 1973.

"On the Feasibility of Software Certification;" Keirstead, R. E.; Stanford Research Institute Project 2385 for National Science Foundation (Grant No. GJ 36903x1).

"Quantitative Aspects of Software Validation;" Rubey, R. J.; Proceedings of International Conference on Reliable Software; Pgs. 245-251; IEEE; April 1975.

"Software Requirements Analysis;" Kassiakoff, A., Sleight, T. P.; Paper presented at Conference on Software Management in Defense Systems and Other Federal Programs; ACM/IEEE; 1976.

"System Simulation;" Gordon, G.; Prentice-Hall; Englewood Cliffs, N. J.; 1969.

"Systems Management Applied to Large Computer Programs in BUIC III; Review of Experience;" Searle, L. V., Rosove, P. E., Sydow, E. H.; ESD-TR-69-302; Air Weapons Surveillance and Control SPO; USAF (ESD); Bedford, Ma.; 1969.

"The Program Development Process;" Aron, J. D.; Phillipines: Adison-Wesley; 1974.

"Verification and Validation of Defense and Space Systems Software;" #76.6455.11-002; TRW; June 1976.

APPENDIX C - REFERENCES*

REGULATIONS, SPECIFICATIONS, AND STANDARDS

[1] AFR 80-14, and AFSC Supplement 1

[2] AFR 800-4

[3] AFR 800-14, Volume II

[4] AFR 800-19

[5] AFSCR/AFLCR 80-17

[6] Deleted

[7] AFSCP 800-3

SOFTWARE ACQUISITION MANAGEMENT GUIDEBOOKS (see Preface)

[8] Software Maintenance

[9] Software Development and Maintenance Facilities

[10] Life Cycle Events

[11] Software Documentation Requirements

[12] Verification

[13] Configuration Management

*References appear in text as follows: "see Ref. [11]."

COMMENT SHEET

Software Validation & Certification Guidebook

Reviewer's Name: Reviewer's Organization:

Comments:

Please return to: Hq ESD/MCIT (Stop 36)
Hanscom AFB, MA 01731

(FOLD)

(FOLD)

FROM _____

_____

_____

HQ ESD/MCIT

Stop 36

Hanscom AFB, MA 01731